Morgan Lewis Technology May-rathon 2018

Morgan Lewis is proud to present Technology May-rathon, a series of tailored webinars and in-person programs focused on current technology-related issues, trends, and legal developments.

This year is our 8th Annual Technology May-rathon and we are offering over 30 in-person and virtual events on topics of importance to our clients, including privacy and cybersecurity, new developments in immigration, employment and tax law, fintech, telecom, disruptive technologies, issues in global tech, and more.

A full listing of our Technology May-rathon programs can be found at https://www.morganlewis.com/topics/technology-may-rathon

Tweet **#techMayrathon**

Disclaimer

- Please note that none of the information addressed in written or verbal form should be relied upon as legal advice. Instead, consult an attorney that can provide legal advice based on the specifics of your situation.

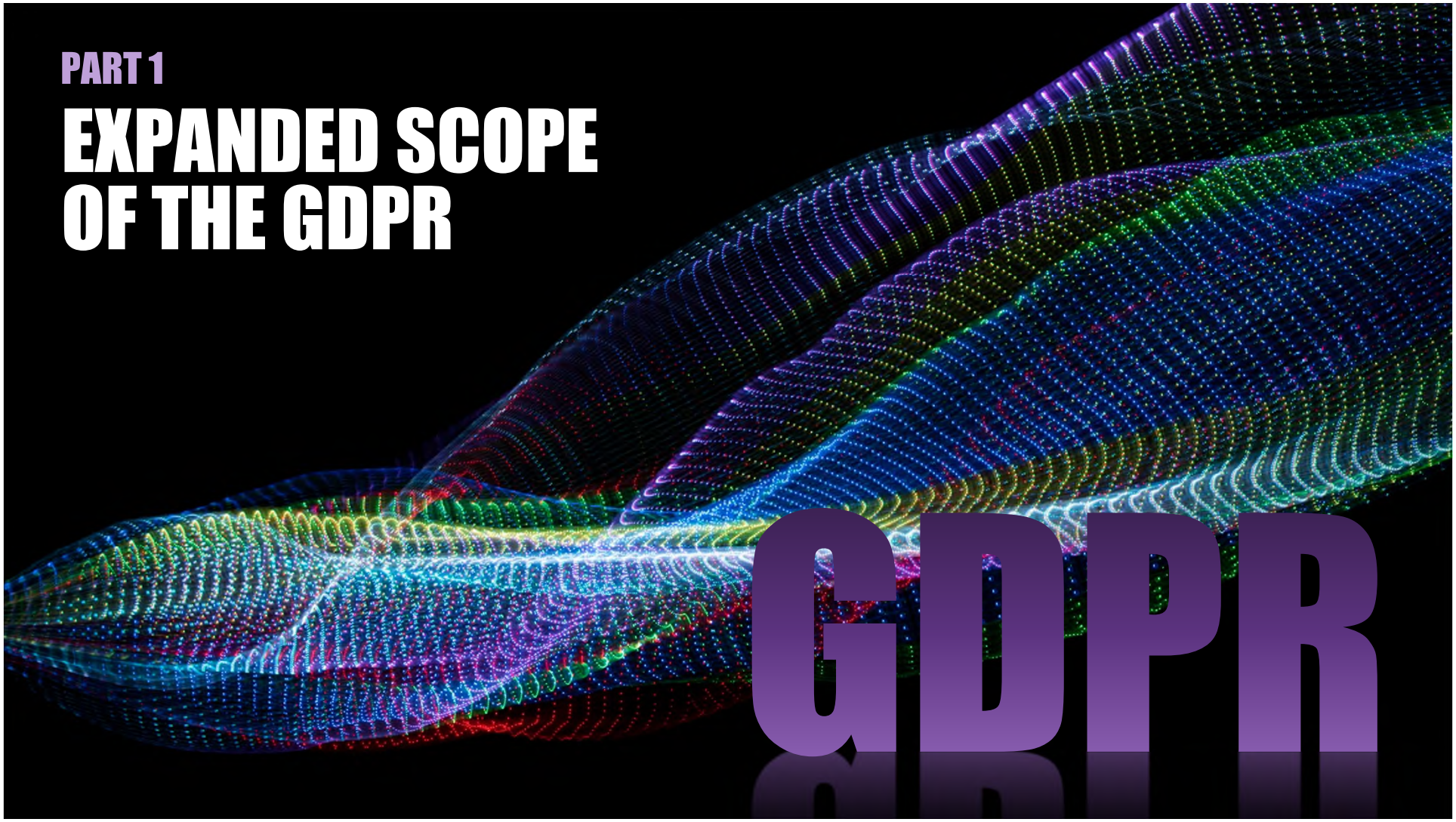
- None of the views expressed in writing or verbally represent the views of the firm or any firm clients. All the views expressed in writing or verbally are those of the presenters.

What's New Under the GDPR?

- Expanded scope
- Security breach notification obligations
- Notice and consent under the GDPR
- New compliance obligations (Data Protection Officer, Data Privacy Impact Assessments, Recordkeeping)
- GDPR Enforcement Risk (individual lawsuits)
- Cross-border data transfers
- Key Takeaways

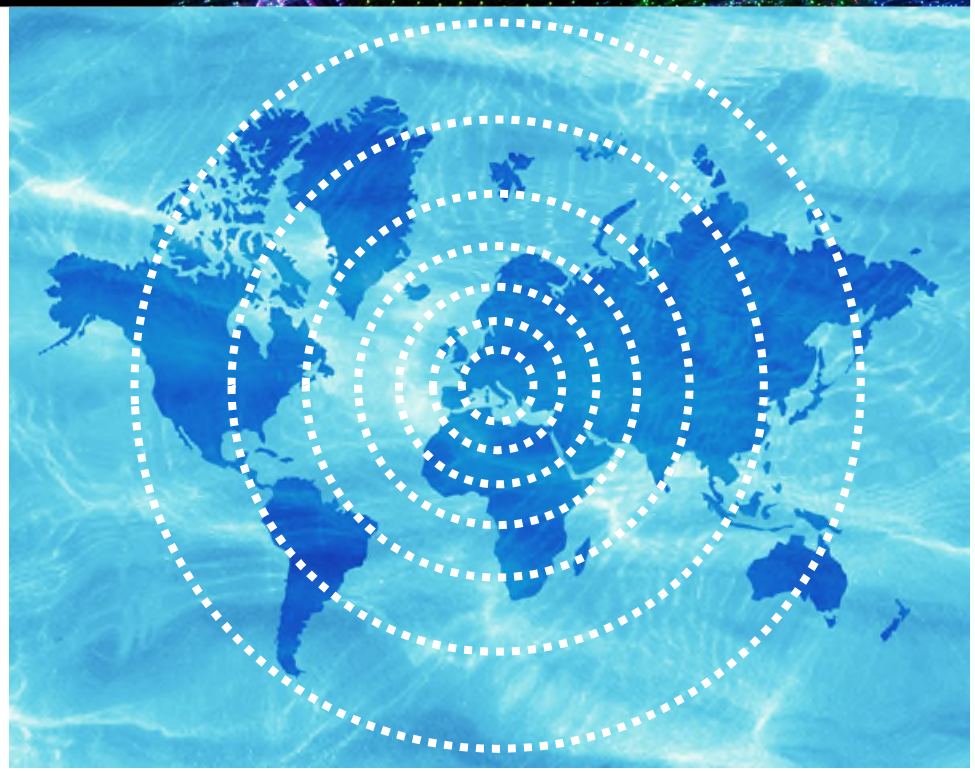
PART 1

EXPANDED SCOPE OF THE GDPR



Expanded Scope of the GDPR

- Penalties and enforcement
- Applies directly to both controllers and processors
  - Obligations
  - Enforcement/Penalties
- Applies to processing of personal data of any individual in the EU
  - Nationality or citizenship of the individual is not relevant



Article 3 – Expanded Territorial Scope of the GDPR

- Applies to entities "established" in the EU
- Applies to entities not established in the EU if the non-EU entity engages in certain activities
- May still be applicable if receiving/processing EU "personal data" for entities subject to GDPR

Article 3(1) – "Establishment" in the EU

- Applies in the context of activities of controllers and processors established in the EU
  - "Effective and real exercise of activity through stable arrangements"
  - An entity's "main establishment" need not be in the EU
  - E.g., Presence of a branch or subsidiary
  - E.g., Presence of a representative
  - E.g., Bank account in a Member State
- Location of data processing is not relevant

Article 3(2) – Entities Not Established in the EU

- (a): "Offering of goods or services . . . to . . . data subjects in the" EU
  - Are you targeting goods/services to the EU?
  - Free or paid not relevant
  - Website accessible from EU not determinative
  - Viewed from data subject's perspective

- (b): Monitoring behavior of data subjects within the EU
  - Recital 24: "*it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person*"
  - Behavior must be in the EU to trigger Art. 3(2)(b)
  - Not limited to "profiling" (i.e., automated decision-making)

Indirect Application of GDPR

- Application of GDPR indirectly through contractual relationships
- May be applicable if processing data on behalf of controller or processor subject to GDPR
  - Controllers must pass through obligations to processors
  - Processors must pass through obligations to sub-processor(s)
  - Indemnification clauses
  - Joint and several liability


PART 2
DATA BREACH
UNDER THE GDPR
GDPR

Data Breach Under the GDPR

- "Personal data breach" is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."
- In the event of a breach, GDPR requires:
  - Notification to the Supervisory Authority;
  - Without undue delay, and where feasible no later than 72 hours; and
  - May also trigger notification obligations to affected data subjects

- Important Exception: No notification required if the "personal data breach is unlikely to result in a risk for the rights and freedoms of natural persons"

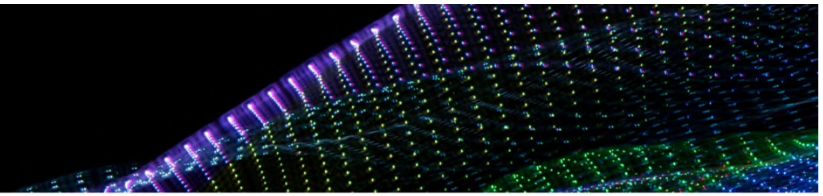
Data Breach Notification Obligations

- There are detailed formal requirements for the notification to a supervisory authority. The notification must at least:
  - Describe the nature of the personal data breach, including the categories and number of data subjects concerned, and the categories and approximate number of data records concerned
  - Communicate the identity and contact details of the DPO or other contact point where more information can be obtained
  - Describe the consequences of the personal data breach
  - Describe the measures proposed or taken by the controller to address the personal data breach

PART 3

GDPR NOTICE AND CONSENT OBLIGATIONS

Data Protection Principles



- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

New Rights Granted to Individuals

- Right to be erasure
- Right to data portability
- Right to be informed
- Right of access
- Right to rectification
- Right to restrict processing
- Right to object
- Rights related to automated decision making including profiling

More Detailed Notice Obligations

- Right to be informed about the collection and use of personal data
- Concise, transparent, intelligible, easily accessible, and it must use clear and plain language
- Must provide individuals with information, including purposes, retention periods, and third-party sharing information
- Must provide privacy information to individuals at time of collection of personal data
- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data, and no later than one month
- New uses of personal data brought to individuals' attention before processing

Lawfulness, Fairness, and Transparency

- Consent
- Necessary for entering into or performing a contract
- Compliance with a legal obligation to which the data controller is subject
- Necessary to protect the vital interests of the data subject
- Direct marketing (requires prior consent)
- Fraud prevention

Obtaining Consent under the GDPR

- Consent remains a lawful basis to transfer personal data under the GDPR
- Under the EU Privacy Directive – "opt-out" consent allowed in some circumstances
- GDPR requires the data subject to signal agreement by "a statement or a clear affirmative action"

Obtaining Consent under the GDPR (cont'd)

- Distinct requirements for processing "special categories of personal data" remain, but expands the range
- GDPR introduces restrictions on the ability of children to consent to data processing without parental authorization
- Whenever a controller relies on consent as a basis for processing, the controller bears the burden of demonstrating that consent was obtained lawfully

Obtaining Consent under the GDPR (cont'd)

- Form of Consent:
  - Affirmative action (no more opt-out; pre-checked boxes, etc.)
  - Segregated – separately highlighted and distinguishable
  - Granular - separate consent should be sought for different types of processing
  - Identified – each entity to which the data subject is consenting is identified
  - Evidence – controller must demonstrate effective consent obtained from data subject
- Withdrawal of Consent: Data subject has the right to withdraw consent at any time
- Freely Given Consent: For the majority of data processing at work, the lawful basis cannot and should not be the consent of the employees due to the nature of the relationship between employer and employee.

Obtaining Consent under the GDPR (cont'd)

- Purpose Limitation: Binds the data controller to the specified, explicit and legitimate purposes notified to the data subject on collection of the personal data.
- Exceptions:
  - Further processing with the data subject's consent
  - Further processing on the basis of an EU or Member State law
  - Further processing for public interest purposes
- Further Compatible Processing:
  - Nexus between disclosed purpose initially and intended purpose for further processing
  - Context in which the personal data has been collected; relationship between the data subjects and controller
  - Nature of personal data and whether special categories of personal data are processed
  - Possible consequences of the intended further processing for data subjects
  - Existence of appropriate safeguards, which may include encryption or pseudonymisation

PART 4

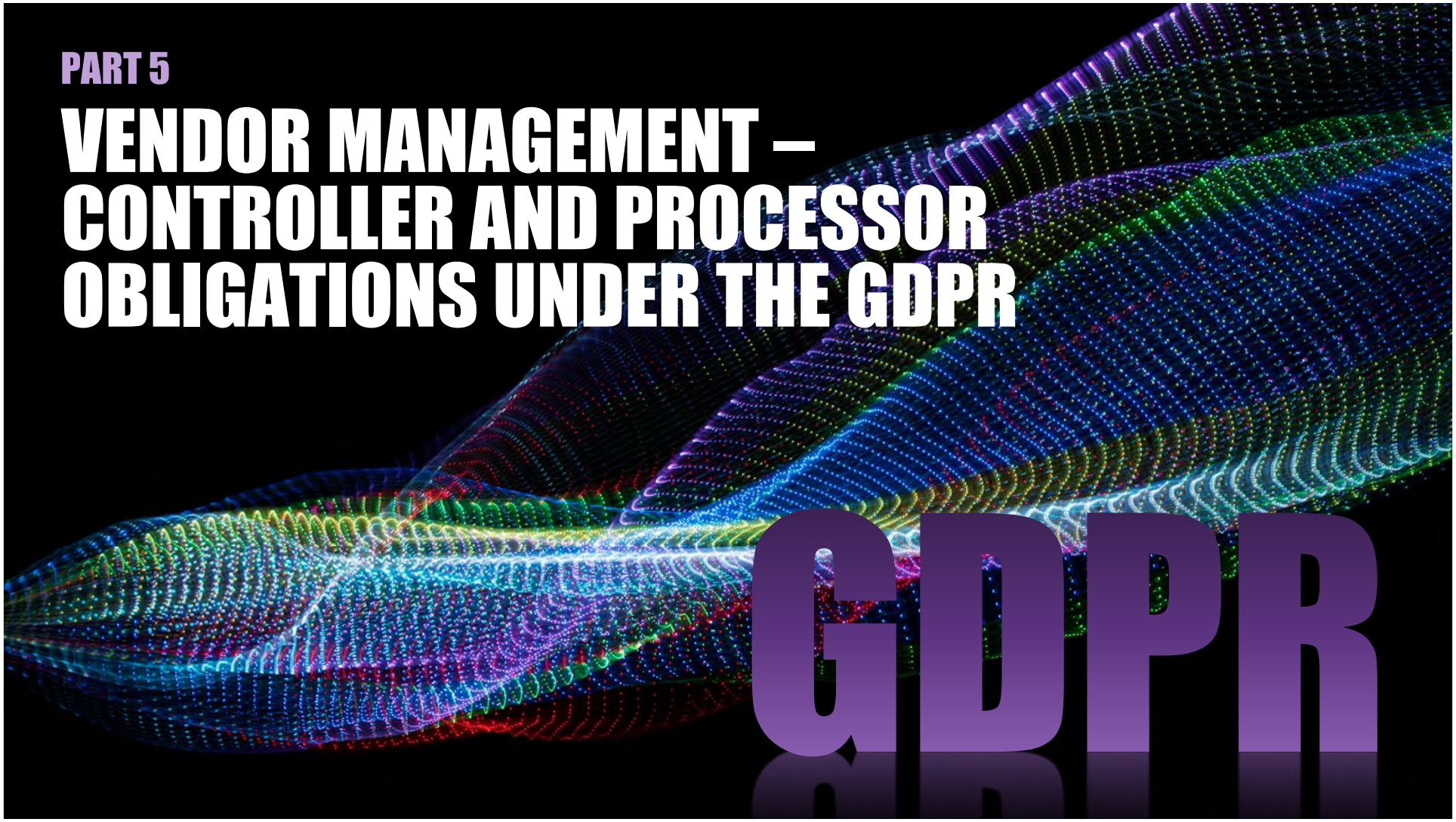
GDPR COMPLIANCE OBLIGATIONS

Introduces New Compliance Obligations

- Data Protection Officer –
  Applies to controllers and processors
- Recordkeeping requirements –
  Imposed on controllers and processors
- Data security
- Data protection by design
- Data protection by default
- Codes of conduct and certification mechanisms
- Data protection impact assessment

Data Protection Impact Assessments (DPIAs)

- Data controllers must conduct DPIA under certain situations
  - Profiling, evaluating, or scoring data subjects (e.g., for predictive purposes)
  - Automated decision making
  - Systematic monitoring
  - Processing sensitive data, or data of a highly personal nature
  - Large-scale data processing
  - Matching or combining data sets
  - Processing data concerning vulnerable data subjects


PART 5
VENDOR MANAGEMENT – CONTROLLER AND PROCESSOR OBLIGATIONS UNDER THE GDPR
GDPR

Controllers Must Ensure the Processing of Personal Data Complies with Certain Principles

- Lawfulness, fairness and transparency – Imposes a disclosure obligation such that data subjects are informed as to what their personal data will be used for;
- Purpose limitation - Personal data must be collected only for an explicit purpose and not be subject to additional processing that would be inconsistent with the specified purpose;
- Data minimization - Only process personal data actually needed to achieve stated purpose;
- Accuracy - Personal data must be accurate and kept up to date. Inaccurate personal data should be corrected or deleted;
- Retention – Stored for no longer than is necessary to achieve the processing purpose;
- Data Security- A number of obligations considered in prior two slides; and
- Accountability – Must be able to demonstrate compliance with data protection obligations.

Cloud Computing and the GDPR

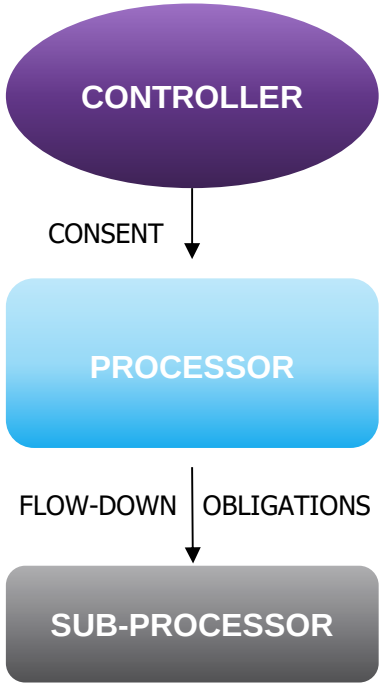
- Delivery Models:
  - Infrastructure as a Service
  - Platform as a Service
  - Software as a Service
- Service Delivery Options:
  - Public clouds
  - Private clouds
  - Hybrid clouds
  - Managed clouds
- Legal Issues:
  - On-demand sub-contracting
  - Traditionally, non-negotiable contractual terms
  - Privacy and data security

Using Third-Party Data Processors

- Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures.
- The processors shall not engage another processor (sub-processors) without prior specific or general written authorization of the controller. In the case of general written authorization, the processors shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Selected Processor Obligations

- Processor must not appoint a sub-processor without the prior written consent of the controller. Sub-processors must be subject to flow-down obligations from the processor.
- Processor is subject to confidentiality obligations and personnel must have same.
- Processor (and any sub-processors) shall not process personal data, except in accordance with the instructions of the controller, or the requirements of EU law or the national laws of Member States.



Selected Processor Obligations

- Recordkeeping obligations
- Cooperate with Data Protection Authorities
- Data security obligations
- Data breach reporting
- Appointment of a Data Protection Officer (if applicable)
- Cross-border transfers

Controller and Processor Data Security Obligations

- Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of processing, as well as the risk associated with the nature of the personal data collected, the controller and the processor must implement "appropriate technical and organizational measures" to ensure a level of security appropriate to the risk, which may include:
- Pseudonymisation/Encryption of personal data;
- Business continuity (backup and redundancy);
- Regularly assessing, evaluating, and testing of such technical and organizational measures;
- Privacy by Design;
- Privacy by Default.
- Adherence to an approved Code of Conduct may provide evidence that the controller and processor have satisfied these obligations.

Data Processor Contracts: Mandatory Provisions

- Scope, nature and purpose of processing must be defined
- Identify types of personal data to be processed
- Duration of the processing
- Processes the personal data only on documented instructions from the controller
- Data security obligations must be addressed
- Processor must assist controller in meeting its obligations regarding data breaches

Data Processor Contracts: Mandatory Provisions (cont'd)

- Processor must assist controller in satisfying requests from data subjects
- Processor must return or delete personal data at end of contract
- Demonstrate compliance with all of the obligations imposed by the GDPR
- Allow the controller to perform compliance audits
- Consent of the controller is required if processor uses a sub-processor
- Flow-down obligations imposed on sub-processor
- Independent obligation to inform the controller if, in its opinion, the controller's instructions would breach Union or Member State law

PART 6

GDPR ENFORCEMENT BY REGULATORS AND THIRD PARTIES: AN UNDERREPORTED TOPIC

Joint Liability

- Article 26(3)
  - The data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers.

- Article 82
  - Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

GDPR Enforcement Risk by Regulators in the EU

- **May 26, 2018**: What to expect from the EU regulators (DPAs)?
- Staffing issues at the EU regulators
- Potential "high-value" targets?
- Future role of the lead DPA (Art. 60) and mutual assistance (Art. 61)
- Future role of the new EU Data Protection Board (Art. 64, 65, 68).

GDPR Enforcement Risk (individual lawsuits)

- **Legal Basis for Individual Law suits :** Art. 82 (1) GDPR: "*Any person who has suffered material or non-material damage as a result of an infringement of this Regulation [GDPR] shall have the right to receive compensation from the controller or processor for the damage suffered.*"
- **What is covered?** All individual rights under the GDPR, such as
  - Documentation obligations (Art. 30)
  - Obligations to delete and correct data (Art. 16, 17)
  - No, false or late notification of a data security breach (Art. 32)
  - Violation of the information rights benefitting the data subjects (Art. 12)

GDPR Enforcement Risk (individual lawsuits) (cont'd.)

- **Who can raise the claim?**
  - The data subject who suffered the damage (Art. 4)
  - Family members and other in case of immaterial damages (possible, but rare)
- **Who is the target of the claim?**
  - The data controller as the primary target (Art. 4 (7)) – this includes any violation of its duty to supervise the data processors.
  - Any data processor as the secondary target (Art. 4 (8), 82 (2) – if he violates his specific duties under the GDPR.

  - Both will be jointly and severally liable under the GDPR.
  - There is no specific EU court for these claims (national civil litigation).

GDPR Enforcement Risk (individual lawsuits) (cont'd.)

- **What damages can be claimed?**
  - Scope (material and immaterial damages depends, on national (e.g., German) law.
  - Potential damages (under general German case law)
    - **"*Material" damages*** caused in and on devices of the claimant, but not the mere data loss alone. Likely covered: device replacement, loss of value of a shareholding, funds necessary to restore a reputation, higher fees due to lower credit ratings, costs of credit monitoring, exchange of credit cards, legal fees, etc.
    - **"*Immaterial" damages*** such as loss of reputation, psychological and mental consequences caused by a data breach (national tort law determines the scope and the causality).

GDPR Enforcement Risk (individual lawsuits) (cont'd.)

- There is **no cap for damages** in Art. 82.
  - There are no charts that German judges use, and not much case law.
  - Current damage levels are typically €1,000 to €7,000 per data subject and incident, but the amount can be much higher in severe cases.

→ The high penalties that the DPAs can impose against companies for GDPR violation do not necessarily "flow down" to the data subjects and impact their claims, but …

→ Indirectly, they may likely lead to a much higher level of damages that a data subject can possibly recover under Art. 82 GDPR.

GDPR Enforcement Risk (individual lawsuits) (cont'd.)

- The damage assessment may depend on the
  - Severity of the infringement
  - Its scope and amount of damage inflicted
  - Measures of the company to mitigate the damage, and
  - The willingness of the company to cooperate with the authorities.

→ An **EU- wide "catalogue" for judges and regulators to calculate damages** under Art. 82 is highly desirable but not likely.

→ Usually the judge will assess the damage individually (there will be no jury trial).

GDPR Enforcement Risk (individual lawsuits) (cont'd.)

- **Who bears the burden of proof?**
  - Data subjects have extensive **information rights** against data controllers to inquire about their data processing (Art. 15)
  - **Accountability principle** under the GDPR: Every data controller must prove that all data processing is fully documented and fully complies with the GDPR.
  - This principle may lead to a shift in the burden of proof for violations, in some cases benefiting the data subjects.

    → Sufficient that the data subject asserts a claim and prove that the data controller has processed his personal data.

GDPR Enforcement Risk (individual lawsuits) (cont'd.)

- Mere **external audits** and ISO compliance are currently not sufficient to exonerate the data controller.
- The Company will need to prove as part of the proceeding that it has **fully complied with all duties of care** and,
- Remains responsible for any processor it has involved. It cannot exonerate itself by stating it has properly supervised the data processor.
- The company may claim that there is **no causality** between the violation and the damage.

GDPR Enforcement Risk (individual lawsuits) (cont'd.)

- **Are class actions possible under Art. 82 GDPR?**
  - Class actions are currently rare under European (German) law. Art. 80 GDPR states that the "*data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State […] to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.*"
  - In Germany, "class actions" under Art. 82 will be more difficult than in the US.
  - General risk that "professional litigators" will highjack this process, e.g., by triggering and managing grass root petitions online.

GDPR Enforcement Risk (individual lawsuits) (cont'd.)

- Legal proceedings in court as **test cases** are always possible.
- Data subjects could also raise their **claims with the DPAs** that would then, after their own investigation, impose fines and/or open their files to the data subjects and others under the national freedom of information acts and general administrative law.
- Legal experts in Germany expect an upswing in **GDPR-related** litigation.


PART 7
CROSS-BORDER TRANSFERS AND THE GDPR
GDPR

Cross-Border Transfers and the GDPR

- GDPR restricts transfers of personal data outside the EU
- Allowed if:
  - Adequacy Decision
  - Binding Corporate Rules
  - Standard Contractual Clauses
  - Certifications
  - Approved Code of Conduct
  - Ad Hoc contractual clauses
  - Derogations (e.g., explicit consent from the data subject)
  - Privacy Shield


PART 8
Key Takeaways
GDPR

Key Takeaways

- Know your **data flows** within and between your organization
- Determine whether the **GDPR applies** to your US organization
- **Revisit privacy policies** (new consent requirements, disclosures)
- GDPR-compliance **data breach notification** (update/establish internal procedures)
- Revisit each **data transfer agreement(s) with vendors and subsidiaries** (Ask: Are GDPR amendments needed?)

Key Takeaways (cont'd.)

- **Audit trails** (e.g., for individual consents) to cover potential litigation/inquiries.
- Designate a **Data Protection Officer and a Data Protection Representative** where required.
- Set up **internal data processing register** (Think about: Who administers it? What is the reporting line?).
- Set up **tools** for external inquiries.

Biographies

Ronald W. Del Sesto, Jr.
Washington, DC
T +1.202.373.6023
E ronald.delsesto@morganlewis.com

Ronald W. Del Sesto, Jr. is a partner in the telecommunications, media, and technology (TMT) practice group. Ron's practice concentrates on the representation of technology companies on a broad range of issues including corporate, financial, regulatory, and cybersecurity. Ron also advises financial institutions, private equity firms, and venture capital funds with respect to investments in the TMT sectors.

Biographies

Dr. Axel Spies
Rechtsanwalt, Special Legal Consultant
Washington, DC
T +1.202.373.6145
E axel.spies@morganlewis.com

Dr. Axel Spies advises domestic and international clients on international legal issues, such as licensing, competition, corporate issues, and new technologies such as cloud computing, in the European markets. He counsels on international data protection, international data transfers, privacy, technology licensing, e-discovery, and equity purchases. He is also a co-publisher of two German journals "ZD" (Journal for Data Protection) and "MMR" (Multimedia Law).

Biographies

Patricia Cave
Associate
Washington, DC
T +1.202.793.5767
E patricia.cave@morganlewis.com

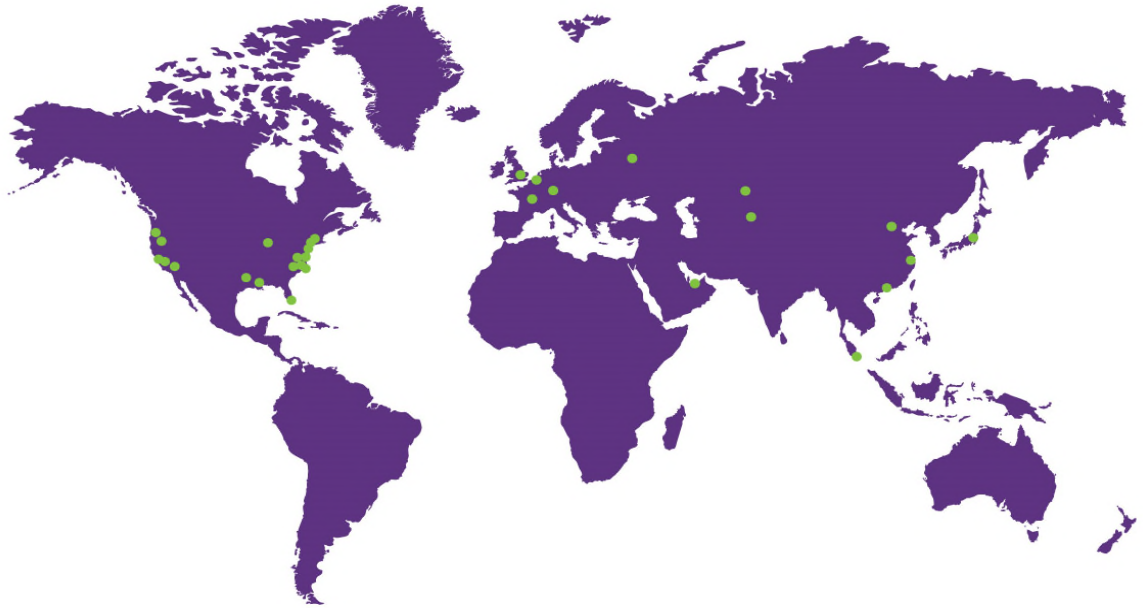
Patricia Cave is an associate in the telecommunications, media, and technology (TMT) practice group. Patricia's practice includes representation of telecommunications and technology companies on a broad range of issues, including corporate, regulatory, data protection, and universal service issues. Patricia also advises clients on international legal issues, such as licensing and infrastructure deployment. Patricia also assists in advising financial institutions, private equity firms, and venture capital funds with respect to investments in the TMT sectors.

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty
Astana
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
Moscow
New York
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore
Tokyo
Washington, DC
Wilmington



Morgan Lewis

*Our Beijing and Shanghai offices operate as representative offices of Morgan, Lewis & Bockius LLP. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners.

THANK YOU

Morgan Lewis